CLAIMS

What is claimed is:

1. A method comprising:

comparing at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present.

2. The method of claim 1, wherein comparing at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present comprises:

comparing at least a subset of information received in a security report from a legitimate access point with information previously stored to determine if a rogue access point is present.

3. The method of claim 1, wherein comparing at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present comprises:

comparing at least a subset of client network traffic received with information previously stored to determine if a rogue access point is present.

4. The method of claim 1, further comprising:

initiating countermeasures against rogue access points determined to be present.

5. The method of claim 4, wherein initiating countermeasures against rogue access points determined to be present comprises:

denying of service to rogue access points and/or clients connected to rogue access points determined to be present.

6. An electronic appliance, comprising:

a network interface to receive information; and

a security engine coupled with the network interface, the security engine to compare at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present.

7. The electronic appliance of claim 6, wherein the security engine to compare at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present comprises:

the security engine to compare at least a subset of information received in a security report from a legitimate access point with information previously stored to determine if a rogue access point is present.

8. The electronic appliance of claim 6, wherein the security engine to compare at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present comprises:

the security engine to compare at least a subset of client network traffic received with information previously stored to determine if a rogue access point is present.

9. The electronic appliance of claim 6, further comprising the security engine to initiate countermeasures against rogue access points determined to be present.

10. The electronic appliance of claim 9, wherein the security engine to initiate countermeasures against rogue access points determined to be present comprises:

the security engine to deny service to rogue access points and/or clients connected to rogue access points determined to be present.

11. A storage medium comprising content which, when executed by an accessing machine, causes the machine to implement a security agent in the accessing machine, the security agent to compare at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present.

12. The storage medium of claim 11, wherein the content to compare at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present comprises content which, when executed by the accessing machine, causes the accessing machine to compare at least a subset of information received in a security report from a legitimate access point with information previously stored to determine if a rogue access point is present.

13. The storage medium of claim 11, wherein the content to compare at least a subset of information received from a wired network device with information previously stored to determine if a rogue access point is present comprises content which, when executed by the

accessing machine, causes the accessing machine to compare at least a subset of client network traffic received with information previously stored to determine if a rogue access point is present.

14. The storage medium of claim 11, further comprising content which, when executed by the accessing machine, causes the accessing machine to initiate countermeasures against rogue access points determined to be present.

15. The storage medium of claim 14, wherein the content to initiate countermeasures against rogue access points determined to be present comprises content which, when executed by the accessing machine, causes the accessing machine to deny service to rogue access points and/or clients connected to rogue access points determined to be present.

16. An apparatus comprising:

a wireless access point configured to generate a security report containing at least a subset of information received from other access points.

17. The apparatus of claim 16, wherein the wireless access point complies with the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.11 specification.

18. The apparatus of claim 16, further comprising the wireless access point to transmit the security report to a networked device.

19. The apparatus of claim 16, wherein the security report contains one or more of a media access control (MAC) address, a service set identification (SSID), a radio frequency (RF) band, a RF channel, and/or a signal strength.